

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

DOMINIC C. DZWONCZYK,

Defendant.

4:15-CR-3134

MEMORANDUM AND ORDER

This matter is before the Court on the defendant's motion to suppress evidence ([filing 37](#)), the Magistrate Judge's Findings and Recommendation ([filing 56](#)) recommending that the motion be denied, and the defendant's objection ([filing 59](#)) to the findings and recommendation. Having conducted a de novo review of the record pursuant to [28 U.S.C. § 636\(b\)\(1\)\(C\)](#), the Court will adopt the Magistrate Judge's recommendation. Accordingly, the defendant's objection ([filing 59](#)) will be overruled, and the defendant's motion to suppress ([filing 37](#)) will be denied.

I. BACKGROUND

This case arises from an FBI investigation into online child pornography.¹ The investigation focused on a website called Playpen, which was accessible to users through the "Tor" network. In 2015, the FBI—pursuant to a warrant—seized control of the server supporting that website. Rather than shutting the website down, the agents continued to operate it out of a government facility in Virginia in an attempt to identify and prosecute administrators and users throughout the country. To this end, the FBI requested authorization from a magistrate judge for the use of a Network Investigative Technique, or "NIT"—software that the government could deploy onto the computer of any person who successfully logged on to the Playpen website. Once on a user's computer, the software would transmit certain identifying information about that user back to the FBI—and, in doing so, reveal the user's public IP address. The FBI would then use that

¹ The details of the investigation are not materially disputed. Many of the facts described below derive from the warrant application—specifically from the affidavit in support of the warrant sworn to by FBI agent Douglas Macfarlane. See [filing 40](#).

information to track the physical location of the user, and to secure a search warrant for that user's home or property.

The defendant, through the username "RebeckaBecka," allegedly visited the Playpen website while it was in the government's control. [Filing 66 at 6](#). Using the NIT software, the government uncovered the defendant's IP address, which led them to Cox Communications—an internet provider that services areas in and around Bellevue, Nebraska. [Filing 66 at 6](#). Cox indicated that the IP address was assigned to the defendant, and on August 14, 2015, authorities secured a search warrant for the defendant's home. [Filing 66 at 6](#). The search uncovered child pornography on the defendant's computer.

The defendant has moved to suppress all evidence obtained from the search of his residence and the computers therein. In support of his motion, the defendant argues that the NIT warrant was issued in violation of [Fed. R. Crim. P. 41](#) and [28 U.S.C. § 636\(a\)](#). See [filing 38 at 4-8](#). Relatedly, the defendant argues that, given the nature of the Rule 41(b) violation, the *Leon* good faith exception does not apply. [Filing 38 at 10](#).

After thoroughly reviewing the relevant facts and law, Magistrate Judge Zwart recommended that this Court deny the defendant's motion to suppress. [Filing 56 at 20](#). The defendant filed a timely objection to the Magistrate's Findings and Recommendation, renewing his argument that the evidence was seized in violation of the Federal Rules of Criminal Procedure. [Filing 59](#).

Before addressing the merits of the defendant's objection, the Court will examine the relevant facts in more detail.

1. PLAYPEN & THE TOR NETWORK

Playpen was an internet website that was designed and utilized for the advertisement and distribution of child pornography. [Filing 40 at 15](#). The website also included features whereby users could discuss "matters pertinent to child sexual abuse, including methods and tactics . . . use[d] to abuse children, . . . [and] to avoid law enforcement detection while perpetrating online child sexual exploitation crimes[.]" [Filing 40 at 15](#). Administrators and users routinely utilized the website to send and receive illegal child pornography. [Filing 40 at 15](#).

Playpen operated as a hidden service on an anonymity provider called the "Tor" network. [Filing 40 at 15](#). As explained in the Magistrate's Judge's Findings and Recommendation, hidden services on the Tor network are not typically accessible through traditional internet searches. [Filing 56 at 1](#). So, a user could not, for example, locate or access Playpen through a standard Google or Yahoo search. Rather, a user of the site must (a) have access to the

Tor network, and (b) know the Tor network address for Playpen. *See*, [filing 56 at 1](#); [filing 40 at 17](#). Thus, as set forth in the application for the NIT warrant, accessing Playpen "requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon . . . [Playpen] without understanding its purpose and content." [Filing 40 at 17-18](#).

The value of the Tor network lies in the anonymity it provides its users. To this end, the Tor software "bounc[es users'] communications around a distributed network of relay computers run by volunteers all around the world[.]" *See*, [filing 56 at 2](#); [filing 40 at 16](#). These relay computers are known as "nodes," and an "exit node" is the last computer through which a user's communication is routed. [Filing 56 at 2](#); [filing 40 at 16](#). So, when a user on the Tor network accesses a website, it is the IP address of the "exit node"—not the user—that appears on the site's IP log. *See* [filing 40 at 16](#). Thus, the process is designed to mask the user's actual IP address so that the user remains, to the extent possible, completely unidentifiable. [Filing 40 at 16](#).

2. THE WARRANTS

(a) The NIT Warrant

In December 2014, the FBI received information regarding the possible owner of the IP address associated with Playpen. *See* [filing 40 at 26-27](#). Based on this information, the FBI, in January 2015, obtained and executed a search warrant to seize Playpen's host server. [Filing 40 at 27](#). After reviewing the contents of the server, and confirming its association with Playpen, the FBI cloned the server on a government server in the Eastern District of Virginia. [Filing 40 at 27](#). The administrator of that server was subsequently identified and apprehended.

Rather than shutting down Playpen, the FBI kept operating the site in an attempt to identify and locate other administrators and users of the website. To do so, the FBI, on February 20, 2015, submitted an application for a search warrant, along with a supporting affidavit, to a magistrate judge in the Eastern District of Virginia. *See generally* [filing 40](#). According to the supporting affidavit, the government would "continue to operate [Playpen] from the government-controlled computer server in Newington, Virginia" for a limited period of time, not to exceed 30 days, "in order to locate and identify the administrators and users of [Playpen]." [Filing 40 at 28](#).

But the Tor network, as described above, complicated this investigation by actively masking the IP addresses—and thus the identities—of the website's users. To address this issue, the government sought authorization from the same Eastern District of Virginia magistrate judge to use a Network Investigation Technique, or "NIT," which it would activate on the Playpen website. Once installed, the NIT would deploy onto the computer of any user

who logged on (via username and password) to the Playpen website. [Filing 40 at 31](#). The NIT would then communicate with the computer of the Playpen user, causing the computer to send identifying information back to the FBI. [Filing 40 at 31](#). As described in the warrant application,

In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the [Playpen website], which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the [Playpen website], . . . the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government.

[Filing 40 at 29](#). The information transmitted from the "activating" computer to the FBI via the NIT included: the IP address of the activating computer, and the date and time that the NIT determined the IP address; a unique identifier generated by the NIT to distinguish data from different activating computers; the type of operating system running the computer; information about whether the NIT has already been delivered to the activating computer; the activating computer's operating system username; and the MAC address of the activating computer. [Filing 40 at 30-31](#). The Eastern District of Virginia magistrate judge approved the warrant, authorizing the FBI to deploy the NIT for 30 days. *See* [filing 40 at 3](#).

(b) The Nebraska Warrant

The parties to this dispute agree that, on or around February 28, 2015, the NIT was deployed and attached to a computer with an IP address allegedly belonging to the defendant. *See* [filing 38 at 3](#). Information was gleaned from the defendant's computer, which led the authorities to the defendant's home in Bellevue, Nebraska. The authorities obtained a search warrant (the "Nebraska warrant"), and on August 21, 2015, that warrant was executed on the defendant's home. [Filing 38 at 3](#). Electronic evidence was seized, and an indictment charging the defendant with one count of possession of child pornography and one count of receipt of child pornography was filed on December 8, 2015. [Filing 38 at 3](#).

II. ANALYSIS

The defendant contends that the Eastern District of Virginia magistrate judge, in authorizing the NIT warrant, exceeded the jurisdictional requirements established under the Federal Magistrates Act and Rule 41(b) of the Federal Rules of Criminal Procedure. To this end, the defendant argues that the NIT warrant impermissibly authorized government agents to "seize and search computers located outside the [Eastern District of Virginia.]" [Filing 38 at 4-5](#). And because the NIT warrant exceeded the jurisdictional boundaries of its issuing authority, the defendant argues that it was void, and that the deployment of the NIT therefore amounted to a warrantless search and seizure. Thus, he contends that the government obtained his IP address unlawfully, and then used that information as the basis of probable cause for the subsequent Nebraska warrant. Based on these events, and the nature of the Rule 41(b) violation, the defendant argues that the evidence obtained from his computer (i.e., the pornographic images) must be suppressed.

Before addressing the merits of this argument, the Court will address two separate yet related points. First, it is worth noting that, to the extent the defendant is claiming a violation of his Fourth Amendment rights, that claim is part and parcel of his argument regarding Rule 41(b). In other words, the defendant has not alleged that the warrants were constitutionally deficient under the Warrants clause of the Fourth Amendment *and* issued in violation of Rule 41(b). Rather, his sole claim is that the warrant exceeded the jurisdictional requirements of [Fed. R. Crim. P. 41\(b\)](#), and that the Rule 41(b) violation, at least in part, resulted in a constitutional infirmity.

In advancing this argument, the defendant acknowledges that a violation of Rule 41 is not itself tantamount to a Fourth Amendment violation, and that noncompliance with the Rule does not, in every instance, require suppression. [U.S. v. Spencer](#), 439 F.3d 905, 913 (8th Cir. 2006). In this way, and as discussed in more detail below, the Eighth Circuit distinguishes between Rule 41(b) violations that are "fundamental," thereby necessitating suppression, and those that are "non-fundamental," in which suppression is appropriate only upon a showing of prejudice or reckless disregard of proper procedure. See [United States v. Freeman](#), 897 F.2d 346, 349-50 (8th Cir. 1990); see also [United States v. Jean](#), 2016 WL 4771096, at *17 (W.D. Ark. Sept. 13, 2016). Thus, applying this framework to the facts of his case, the defendant argues that suppression is required because the purported violation of the Rule is fundamental (in that it facilitated a violation of his constitutional rights), and, alternatively, that it resulted in prejudice (in that the search of his home would not have occurred if the Rule had been followed). See, [filing 38 at 8](#); [filing 52 at 2-3](#).

Second, the Playpen investigation has resulted in nationwide litigation, producing largely divergent opinions regarding the validity of the NIT warrant under [Fed. R. Crim. P. 41\(b\)](#), and the applicability, if at all, of the exclusionary rule. With respect to these issues, and as discussed in more detail below, courts have generally reached one of three results: either (1) the NIT warrant was unlawfully issued and suppression is required; (2) the NIT warrant was unlawfully issued, but suppression is not the appropriate remedy; or (3) the NIT warrant was lawfully issued, and there are no legal violations that require suppression. See [United States v. Johnson](#), 2016 WL 6136586, at *3 (W.D. Mo. Oct. 20, 2016) (collecting cases).

Magistrate Judge Zwart, in her Findings and Recommendation to this Court, recommends the third result—that is, that the NIT warrant complied with Fed. R. Crim. P. 41(b), and that there are no legal violations that require suppression. See [filing 56 at 13](#), 16. In reaching this result, Judge Zwart first determined that the deployment of the NIT was not a "search" for purposes of the Fourth Amendment. [Filing 56 at 10](#). She next concluded that, even assuming the NIT was a search, the search warrant was validly issued under Fed. R. Crim. P. 41(b), and even assuming otherwise, that it did not result in a constitutional infirmity or prejudice. [Filing 56 at 10-16](#). And finally, she determined that even assuming the warrant was invalid, and that it caused either a constitutional infirmity or prejudice, that the good faith exception set forth in *United States v. Leon* and its progeny would prohibit suppression of the evidence. [Filing 56 at 17](#).

For the reasons set forth below, the Court adopts the Magistrate Judge's recommendation, and accordingly, will deny the defendant's motion to suppress. However, the Court takes a different path to this result. Specifically, the Court concludes that the NIT warrant was issued in violation of Rule 41(b), and that the government's conduct amounted to a search under the Fourth Amendment. However, consistent with the findings and recommendation, the Court concludes that the Rule 41(b) violation was neither "of constitutional magnitude," or otherwise prejudicial. Further, because the officers acted in reasonable good faith, the Court finds that, even if the violation implicated the exclusionary rule, suppression—at least on these facts—is not the appropriate remedy.

1. FED. R. CRIM. P. 41

The defendant argues that the NIT warrant was issued in violation of [Federal Rule of Criminal Procedure 41\(b\)](#), which, at all relevant times,² provided in part,

(b) **Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property *located within the district*;

...

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both[.]

[Fed. R. Crim. P. 41\(b\)](#) (emphasis added). Specifically, the defendant contends that, pursuant to the Rule, a magistrate judge is powerless to authorize and issue a search warrant for persons, places, or things that are located outside of his or her judicial district. [Filing 28 at 5](#). And because the NIT warrant was issued in the Eastern District of Virginia, but purportedly executed on the defendant's home computer in Bellevue, Nebraska, it is "void ab initio and per se harmful." [Filing 38 at 5](#).

The government argues that the NIT is a "tracking device," and therefore that the magistrate judge in the Eastern District of Virginia had authority to issue the warrant under subpart (b)(4). *See*, [filing 45 at 8-11](#); [filing 66 at 15](#). As noted above, that provision authorizes the use of tracking devices, so long as the device is installed within the magistrate judge's district. And once installed, the tracking device may continue to operate even if the object tracked moves outside of the issuing district. *See* Fed. R. Crim. P. 41(b)(4); *see also* [filing 66 at 15](#).

² As of December 1, 2016, Rule 41(b) is now titled "Venue for a Warrant Application." *See* [Fed. R. Crim. P. 41\(b\)](#). This change, and others, were not in effect at the time of the present investigation.

Consistent with Magistrate Judge Zwart's recommendation to this Court, several courts have determined that the NIT is—or is sufficiently analogous to—a "tracking device," and that the warrant is therefore valid under Fed. R. Crim. P. 41(b)(4). [Filing 56 at 11-13](#); *see, e.g., United States v. Johnson*, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Lough*, 2016 WL 6834003 (N.D. W. Va. Nov. 18, 2016); *United States v. Jean*, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Matish*, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, 2016 WL 3189703 (E.D. Va. June 3, 2016). This position is summarized in *United States v. Jean*.

In *Jean*, the court began its analysis by acknowledging that the FBI was not "seeking to install a tangible tracking device to some other physical piece of property," and as a result, that the NIT does not squarely comport with a traditional understanding of tracking techniques. *Id.* at *16. However, the court noted that "[i]nternet crime and surveillance defy traditional notions of place," and that subpart (b)(4) expressly authorizes the tracking of "property," which the Rule defines to include the tracking of intangible "information." *Id.* at 15-16 (citing Rule 41(a)(2)(A)). Similarly, the court references the definition of "tracking device," which the Rule defines as any "electronic or mechanical device which permits the tracking of the movement of a person or object." *Id.* (citing Rule 41(a)(2)(E), which cross-references this definition from [18 U.S.C. § 3117\(b\)](#)).

Finding that the NIT falls within the definition of "tracking device," and that the device was used to track the movement of "property" (i.e., information), the court then concluded that the third requirement—that the device be "install[ed] within the issuing district"—was also satisfied. On this point, the court remarked,

[T]he term "install" is problematic, primarily because—in a more traditional scenario—the tracking of tangible property under Rule 41(b)(4) requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property—information—something expressly contemplated by Rule 41(a)(2)(A). So when one uses an intangible technique to track the flow of information, to what does the term "install" refer, and where does "installation" take place? Mr. Jean argues that the NIT was downloaded onto his computer, and therefore installation occurred in Arkansas. But that statement isn't entirely correct. While it is obviously true that Mr. Jean and his computer were

never physically present in Virginia, it is equally accurate that the warrant did not violate Rule 41(b)(4)'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device used here.

Jean, 2016 WL 4771096, at *16. Thus, on these facts, the court concluded that "the only reasonable interpretation of where the information-tracking NIT was 'install[ed]' for purposes of Rule 41(b)(4), is the Eastern District of Virginia[.]" *Id.* at 17. Finding all requirements satisfied, the court determined that the Virginia magistrate judge, pursuant to Rule 41(b)(4), had the authority to issue the warrant, and that the resulting seizure of evidence was therefore lawful. *Id.*

Other courts have found Rule 41(b)(4) inapplicable to the NIT warrant. For example, in *United States v. Croghan*, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016), the court determined that the NIT is not a "tracking device" as that term is defined by the Rule. Specifically, the court concluded that, under a "plain meaning" interpretation, the NIT did not "track" the "movement" of anything; rather, "it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia." *Id.* at *4. A contrary holding, the court noted, would cast too broad a net, thereby encompassing investigative techniques not otherwise envisioned by the Rule. *See id.* (citing *United States v. Torres*, 2016 WL 4821223, at *6 (W.D. Tx. Sept. 9, 2016) ("It is inappropriate for this Court to engage in a process of finesse justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of the rule as now written does not provide jurisdiction under these circumstances.")); *see also United States v. Henderson*, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016) ("The NIT search does not meet the requirements of 41(b)(4) because, even though it was analogous to a tracking device in some ways, it nevertheless falls outside the meaning of a 'tracking device' as contemplated by the rule.").

Adding to this position, the court in *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) noted that the application of subpart (b)(4) to the NIT warrant would "stretch[] the rule too far." *Id.* at *6. Even assuming the "installation" occurred on the government-controlled computer in Virginia, the court remarked, Rule 41(b)(4) would not apply because the defendant "never controlled the government-controlled computer." *Id.* Similarly, assuming the installation occurred on the defendant's computer, subpart (b)(4) would still fail because the defendant's computer "was never physically located within the Eastern District of Virginia." *Id.*; *see also, United States v. Werdene*, 2016 WL 3002376, at *7 (E.D. Pa. May 18, 2016)

(holding subpart (b)(4) inapplicable because it is "uncontested that the computer information that the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia"); *Henderson*, 2016 WL 4549108, at *4 ("[T]he NIT was installed outside of the district, at the location of the activating computers, not within the district as required by Rule 41(b)(4).").

After reviewing the plain text of the Rule, and considering the well-reasoned opinions of several federal district courts, the Court finds that the Eastern District of Virginia magistrate judge exceeded the jurisdictional limitations set forth in Rule 41(b).³ In reaching this decision, the Court rejects the argument—for the reasons set forth in *Croghan*, *Henderson*, and *Werdene*—that the NIT was a "tracking device," and that the warrant was therefore valid under subpart (b)(4). Relatedly, the Court concludes that, even assuming the NIT was a "tracking device," it was not "installed" in the Eastern District of Virginia, and therefore was not authorized under the Rule.

As noted above, the term "tracking device" is defined for purposes of Rule 41 as any "electronic or mechanical device which permits the tracking of the movement of a person or object." See Fed. R. Crim. P. 41(a)(2)(E) (adopting the definition of "tracking device" as set forth in 18 U.S.C. § 3117(b)). As noted in *Croghan*, while the term "track" is not further defined, "its ordinary meaning is '[t]o follow up the track or footsteps of; to trace the course or movements of; to pursue by or as by the track left.'" *Croghan*, 2016 WL 4992105, at *4 (citing <http://www.oed.com>).

Applying these definitions to the facts of this case, the Court finds that the NIT is not a tracking device for purposes of the Rule. As set forth in the affidavit in support of the warrant, the NIT, once it attaches to the activating computer, "transmit[s] certain information [from the activating computer] to a computer controlled by or known to the government." See filing 40 at 29. In this way, the value of the NIT lies not in its ability to "track" the "movement" of information (which it does not do), but rather in its capacity to relay information from one computer (the user's) to another (the government's). See *Croghan*, 2016 WL 4992105, at *4. And while the information is ultimately used to track the location of individuals, that broader objective is neither relevant to, nor dispositive of, the underlying analysis.

³ The following analysis also recognizes that the Rules of Criminal Procedure are to be applied flexibly. See, *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977) (Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992).

More fundamentally, though, the Court finds that, even assuming the NIT was a tracking device, it was not "install[ed] within the district" as required under subpart (b)(4). On this point, it is undisputed that the defendant's computer was, at all relevant times, located in Bellevue, Nebraska. And while the defendant allegedly used his computer to access the Virginia server, that electronic activity is not enough, in this Court's view, to bring the defendant within the territorial reach of the Rule. The defendant's computer never left Nebraska, so it was obviously still in Nebraska when the NIT code was downloaded to his computer in Nebraska and executed there. After all, subpart (b)(4) is "premised on the person or property being located within the district," and neither of those requirements are satisfied here. [Werdene, 2016 WL 3002376, at *7](#).

It is also worth noting the recent change to Rule 41, which resulted in the addition of subpart (b)(6). That provision (which went into effect after the Playpen investigation) generally provides magistrate judges authority to issue warrants "to use remote access to search electronic storage media . . . located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means." [Fed. R. Crim. P. 41\(b\)\(6\)](#). The Advisory Committee's records, which highlight the reasoning for the change, note:

The proposal speaks to two increasingly common situations affected by the territorial restriction, each involving remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet. In the first situation, the warrant sufficiently describes the computer to be searched, but the district within which the computer is located is unknown. This situation is occurring with increasing frequency because persons who commit crimes using the Internet are using sophisticated anonymizing technologies . . . [such as] proxy services designed to hide their true IP addresses.

Report of the Advisory Committee on Criminal Rules to the Committee on Rules of Practice and Procedure (May 2015).

This change seems to address the very issue presented in the underlying dispute. And while not dispositive, the change—and the impetus behind it—is instructive. At a minimum, it suggests concern regarding the applicability of Rule 41(b) as previously written to investigations like the one at issue here, and a need to amend the rules accordingly. And for the reasons stated above, those concerns were well-founded—indeed, a plain reading of

the Rule suggests, clearly, that it was simply not written to encompass these kinds of technological advancements.

2. SUPPRESSION

As previously noted, a violation of Rule 41(b) does not, in every instance, trigger the exclusionary rule. Rather, absent a constitutional infirmity, "the exclusionary rule is applied only to violations of Federal Rule 41 that prejudice a defendant or show reckless disregard of proper procedure." *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993); *see also United States v. Welch*, 811 F.3d 275, 280-81 (8th Cir. 2016). So, for the exclusionary rule to apply in this case, the defendant must show, in addition to the Rule 41(b) violation, *either* (1) the violation is of constitutional magnitude; (2) he was prejudiced in that the search would not have taken place or would not have been as intrusive; or (3) evidence of an intentional or reckless disregard for the truth. *United States v. Skarda*, No. 15-3889, slip op. at 6-7 (8th Cir. Dec. 22, 2016) (citing *United States v. Freeman*, 897 F.2d 346, 349-50 (8th Cir. 1990)).

(a) Constitutional Magnitude

The defendant argues that the Rule 41(b) violation at issue rises to the level of a Fourth Amendment violation. [Filing 60 at 8](#). To support this argument, the defendant first contends that he had a reasonable expectation of privacy in the information seized and/or the places searched. *See* [filing 60 at 2-5](#).

(i) Search

The Fourth Amendment provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." [U.S. Const. amend. IV](#). "It is clear that a physical intrusion or trespass by a government official constitutes a search within the meaning of the Fourth Amendment." *United States v. DE L'Isle*, 825 F.3d 426, 431 (8th Cir. 2016) (citing *United States v. Jones*, 132 S. Ct. 945, 949 (2012)). But "[a] search is reasonable if the officer has a valid search warrant or if the search fits within a specific warrant exception." *Id.*

For a "search" to occur within the meaning of the Fourth Amendment, an individual must have a "reasonable expectation of privacy" in the place or thing subjected to search. *Jones*, 132 S. Ct. at 950. "For this type of violation, the claimant must show both an actual (subjective) expectation of privacy and . . . that the expectation [is] one that society is prepared to recognize as reasonable." *De L'Isle*, 825 F.3d at 431 (internal quotations omitted). If a law

enforcement official's search does not offend a person's reasonable expectation of privacy, the Fourth Amendment is not implicated. *Id.*

Magistrate Judge Zwart, in her recommendation to this Court, concluded that the defendant, regardless of his attempt at anonymity through the Tor network, did not possess a reasonable expectation of privacy in his IP address. [Filing 56 at 6-7](#). This conclusion is supported by Eighth Circuit precedent holding that an individual has no reasonable expectation of privacy in certain internet subscriber data, including IP addresses, which are issued by third-party service providers. *See* [filing 56 at 6](#) (citing *United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014)); *see also* *Welch*, 811 F. 3d at 280 n.4 (noting that IP addresses are generated by a third party and assigned by an internet service provider). Underlying this principle is the fact that an individual "necessarily shares the IP address assigned to his computer to and from third parties[.]" [Filing 56 at 7](#). *See also* *United States v. Laurita*, 2016 WL 4179365, *4 (D. Neb. Aug. 5, 2016) ("It is well established that there is no expectation of privacy when an individual sends information to a third party, even where that information is understood to be confidential.") (citing *Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring)).⁴

The defendant does not meaningfully dispute this conclusion. Rather, he claims that the proper Fourth Amendment inquiry is not whether he has a reasonable expectation of privacy in his IP address, but rather, whether he has a reasonable expectation of privacy in his home computer. *See* [filing 60 at 2-3](#). To this end, the defendant argues that there is a meaningful distinction between the government obtaining an individual user's IP address by issuing a subpoena to a third party internet service provider, *see* *Wheelock*, 772 F.3d at 827, and obtaining that same information by "ripp[ing it] directly from the user's computer." [Filing 60 at 3](#). The defendant points the Court to language in *United States v. Croghan*, in which the court remarked,

There is a significant difference between obtaining an IP address from a third party and obtaining it directly from a defendant's computer. If a defendant writes his IP address on a piece of paper

⁴ On this point, the government, citing Judge Zwart's Findings and Recommendation, further notes that the defendant, even through the use of the anonymous Tor network, was "sharing his IP address with others . . . [including] total strangers, to potentially include law enforcement officers." [Filing 66 at 11](#) (citing [filing 56 at 8](#)). The government further highlights that the Tor network expressly warns users that it "cannot solve all anonymity problems," and therefore that the user's true IP address "is not a complete secret." [Filing 66 at 11](#) (citing [filing 56 at 8](#)). But the government did not *obtain* the IP address from any of those third parties.

and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper—even accepting that the defendant had no reasonable expectation of privacy in the IP address itself. Here, Defendants' IP addresses were stored on their computers in their homes rather than in a drawer. Law enforcement has admitted, however, that it had no way to learn Defendants' IP addresses without deploying the NIT and essentially forcing Defendants' computers to relay identifying information to Virginia. While the IP addresses may have themselves been evidence of a crime, Defendants nonetheless had a reasonable expectation of privacy in the locations where the IP addresses were stored, necessitating that law enforcement obtain a valid warrant before searching such locations.

Id. at *7 (citations and emphasis omitted).

In addressing this distinction, the Findings and Recommendation concludes that the IP address is not a "physical component" or a "file residing on [the] computer" like an electronic document or picture. *See* [filing 56 at 9](#) (citing *Jean*, 2016 WL 4771096, at *5). Rather, the IP address is assigned to a user by an internet service provider and maintained "on the internet modem that connects an internet device to the internet." *Id.* So, the NIT "essentially compelled Defendant's computer to produce its IP address (similar to a return address on an envelope) when the NIT instructed the computer to send other information identified in the [NIT] [w]arrant." *Id.*

The Court agrees with the Findings and Recommendation insofar as it suggests that, as a general matter, individuals have no expectation of privacy in their IP address. *See* [Wheelock](#), 772 F.3d at 828; *see also*, [United States v. Carpenter](#), 819 F.3d 880, 887 (6th Cir. 2016); [United States v. Forrester](#), 512 F.3d 500 (9th Cir. 2007). However, the Court finds the reasoning set forth in *Croghan* persuasive, and concludes that the deployment of the NIT was a search under the Fourth Amendment. Specifically, the Court agrees with the contention that, under these facts, the Fourth Amendment inquiry requires an analysis not only of the information obtained, but more fundamentally, the means of obtaining it. To this end, and as applied to the facts of this case, the question is two-fold: (1) whether the defendant had a reasonable expectation of privacy in his IP address, and (2) whether he had a reasonable expectation of privacy in the location where the IP was ultimately discovered—that is, his home computer.

But to contextualize this analysis, it is important to understand how the NIT works. As noted above, the software, as applied here, enabled the

government to identify the users' IP addresses despite their use of an anonymizing network. To do so, the government installed the NIT on the Playpen website via the server located in the Eastern District of Virginia. See [filing 40 at 29](#). Once activated, the NIT targeted Playpen users by sending additional code or "instructions" to their computers. [Filing 40 at 29](#). Thus, once a user successfully logged on to Playpen, the user's computer would receive both content (which enabled him to see the pornographic images), and "instructions" (injected by the NIT). See [filing 40 at 29](#). Once the activating computer "successfully download[ed]" the instructions, the computer then "transmit[ed] . . . information" to the government in Virginia. See [filing 40 at 29](#); see also [Darby](#), 2016 WL 3189703, *5 ("The NIT surreptitiously placed code on [the defendant's] personal computer that then extracted from the computer certain information."). And it is this information—which included the user's IP address, operating system, and MAC address—that the government relied upon to locate the suspect.⁵ See [filing 40 at 30](#). In other words, the NIT injected code that was downloaded to the defendant's computer, searched the defendant's computer for the identifying information sought by the government, and transmitted that information to the government.

The NIT, by its very operation, is therefore distinguishable from a pen register or port mirroring. Those surveillance techniques capture certain identifying information like phone numbers and IP addresses as those communications are sent from point A to point B. See, [Smith v. Maryland](#), 442 U.S. 735 (1979); [United States v. Forrester](#), 512 F.3d 500 (9th Cir. 2007). The operative inquiry under those circumstances, then, is whether the surveilled suspect has an expectation of privacy in the information obtained—that is, in the phone number dialed, or certain identifying information in an e-mail. And the answer to that question, generally speaking, is no. See, [Carpenter](#), 819 F.3d at 888; [Wheelock](#), 772 F.3d at 828;

⁵ It is not clear how the NIT ascertained the activating computer's public IP address: whether, for example, the NIT initiated a process on the activating computer to learn its public IP address, or perhaps whether the government server to which the NIT transmitted information simply logged the public IP address from which the transmission was made. There could be some distinction, for Fourth Amendment purposes, between code that simply causes an activating computer to reveal itself, and code that actually obtains data from the activating computer and sends it to the government. But that distinction is not meaningful under *these* circumstances, because the NIT clearly provided the government with other information that could only have been obtained from the activating computer. And even if the IP address was the only information at issue—and it is certainly the information that the parties are concerned with—the issue is still how the information was obtained. Beating the bushes to flush game is still a "search" of the bushes, even if the strategy is to compel the game to reveal itself.

United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010); *Forrester*, 512 F.3d at 509-11.

But here, the government obtained the defendant's IP address not from a third party provider, but rather from an intrusion into the defendant's computer. See *United States v. Ammons*, 2016 WL 4926438, *4 (W.D. Ky. Sept. 14, 2016). Thus, by operation, this case implicates not only the defendant's privacy interest (or lack thereof) in his IP address, but also his privacy interest on his home computer. And because the defendant possessed a reasonable expectation of privacy in his computer, the government's deployment of the NIT amounted to a search for purposes of the Fourth Amendment. *United States v. Gano*, 538 F.3d 1117, 1127 (9th Cir. 2008) (recognizing that individuals generally have an objectively reasonable expectation of privacy in personal computers); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers[.]").

(ii) *Validity of the Warrant*

As noted above, the defendant does not contend that the NIT warrant was unsupported by probable cause, issued by a non-detached magistrate, or lacked particularity. Rather, he claims that the Virginia magistrate judge issued the warrant in violation of Rule 41(b), and that the nature of that violation implicated "substantial constitutional protections." *Filing 60 at 9*. To this end, he suggests that the provisions of Rule 41(b) are uniquely substantive in nature, in that they address "the authority of the magistrate judge to issue the warrant," as opposed to other provisions of the rule, which "simply [address] the procedures for obtaining and issuing warrants." See *filing 60 at 9* (internal quotations omitted) (citing *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008); *United States v. Levin*, 2016 WL 2596010, at *7-8 (D. Mass. May 5, 2016)).

In advancing this argument, the defendant relies on *United States v. Levin*, which also addressed the validity of the NIT warrant as applied to evidence obtained from the defendant's home computer. In *Levin*, the court concluded that the Virginia magistrate judge issued the NIT warrant in violation of Rule 41(b), and that the violation was substantive (or "fundamental") in nature. On this point, the court remarked—as the defendant argues here—that the violation "involve[d] the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant[.]" *Id.* at *7 (citing *United States v. Glover*, 736 F.3d

509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes a "jurisdictional flaw" that cannot "be excused as a 'technical defect'"). From there, and proceeding on the assumption that the defendant had a reasonable expectation of privacy in the information seized,⁶ the court concluded that the magistrate judge lacked authority—and thus jurisdiction—to issue the NIT warrant, rendering the warrant void ab initio, or the equivalent of "no warrant at all." *Id.* at *12; see also *Croghan*, 2016 WL 4992105, at *6 ("because there would not have been probable cause to issue the [residential] Warrant[] without the information obtained from the NIT Warrant, all evidence seized as a result of the [residential] Warrant[] must be suppressed as fruit of the poisonous tree").

At least four other federal district courts have adopted or otherwise followed this reasoning in *Levin*. See, *Croghan*, 2016 WL 4992105, at *6; *United States v. Workman*, 2016 WL 5791209, at *8 (D. Colo. Sept. 6, 2016); *United States v. Arterbury*, No. 15-cr-182, Clerk's No. 42 (N.D. Okla. Apr. 25, 2016); see also *United States v. Ammons*, 2016 WL 4926438, at *6 (W.D. Ky. Sept. 14, 2016) (holding that the warrant was void, but that suppression was not warranted). Other courts, however, have reached a different result, concluding that the Rule 41(b) violation, if at all, was merely technical or "non-fundamental" in nature. In reaching this conclusion, courts have determined—albeit implicitly—that a violation of Rule 41(b) is fundamental, or of constitutional magnitude, only if the Rule violation implicates the magistrate's impartiality, the probable cause determination, or the particularity of the warrant. For example, the court in *United States v. Ryan Anthony Adams*, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016) remarked,

The Government accurately asserts that the Fourth Amendment does not impose a venue requirement for applying for a search warrant. The Fourth Amendment imposes three requirements: (1) a search warrant must be issued by a neutral magistrate; (2) it must be based on a showing of probable cause, and (3) it must satisfy the particularity requirement. Defendant does not contend that any of these considerations were not met in the application for, and issuance of, the NIT warrant in this case.

⁶ The *Levin* court assumed that the defendant had a reasonable expectation of privacy in the information obtained because the government "waived any argument" that its investigative conduct did not result in a search. *Id.* at *1 n.1.

Id. (internal citation omitted); *see also*, [United States v. Lough](#), 2016 WL 6834003, at *6 (N.D. W. Va. Nov. 18, 2016) ("There was no constitutional violation here. The parties do not argue, nor has any court found, that the NIT warrant lacked probable cause."); [Jean](#), 2016 WL 4771096, at *17 ("[I]f there was any violation of the Rule at all, it was certainly non-fundamental [because] [t]he search warrant was constitutionally sufficient in that it was supported by probable cause and satisfied the particularity requirement."); [United States v. Henderson](#), 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016) ("The NIT Warrant's violation of Rule 41 is technical because the Warrant complies with the Fourth Amendment requirements of probable cause and particularity.").

Similarly, courts have rejected defendants' arguments that a warrant issued in violation of Rule 41(b) is necessarily void, or akin to no warrant at all. On this point, courts have generally noted that, despite the potential for Rule 41(b) violations, magistrate judges nevertheless possess inherent authority to issue warrants. *See Adams*, 2016 WL 4212079, at *6 ("The Court finds that the magistrate judge in the Eastern District of Virginia had the authority to issue search warrants—that is, the inherent power to do so."). Likewise, courts have implied that the NIT warrant cannot be void, because at a minimum, the warrant validly authorized searches within the Eastern District of Virginia. In other words, as the court in [United States v. Stepus](#), 2016 WL 6518427 (D. Mass. Oct. 28, 2016) remarked,

The magistrate judge may have lacked authority to issue a warrant that permitted deployment of the NIT outside of the court's district, but the warrant was not void *ab initio*. The magistrate judge had authority to allow the NIT to be deployed to computers within the court's district and she signed the warrant within that district.

Id. at *2 (internal citations omitted); *see also* [United States v. Anzalone](#), 2016 WL 5339723, at *11 (D. Mass. Sept. 22, 2016).

The Court concludes that the violation of Rule 41(b) is not, as the defendant contends, of "constitutional magnitude." As the Supreme Court has recognized, "the warrant traditionally has represented an independent assurance that a search and arrest will not proceed without probable cause to believe that a crime has been committed and that the person or place named in the warrant is involved in the crime." [Shadwick v. City of Tampa](#), 407 U.S. 345, 350 (1972). These principles derive from the very text of the Fourth Amendment, which provides "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized." [U.S. Const. amend. IV](#).

But, as noted above, the defendant does not contend that the NIT warrant lacked probable cause, was issued by a non-detached magistrate, or failed to satisfy the particularity requirement: deficiencies that the Eighth Circuit has held necessary for a Rule 41 violation to be of constitutional magnitude. *See Skarda*, No. 15-3889, at *7. Rather, he suggests that the nature of the Rule 41(b) violation rendered the warrant void *ab initio*, and that the government's deployment of the NIT therefore amounts to a warrantless search. But this argument overlooks the magistrate judge's inherent power to issue warrants—including the one at issue—on computers within her district. *See, Stepus*, 2016 WL 6518427, at *2; *United States v. Duncan*, 2016 WL 7131475, at *3 (D. Or. Dec. 6, 2016). It further implies that a violation of Rule 41(b) somehow renders that power (or the accompanying warrant) void, which is to read a jurisdictional requirement into the Fourth Amendment that does not currently exist. *See Skarda*, No. 15-3889, at *7.

The Court also rejects the defendant's argument that provisions of Rule 41, for purposes of a suppression analysis, are either "substantive" or "procedural" in nature. *See filing 60 at 9*. Rather, the Court reads the rules of procedure as just that—rules of *procedure*. And while the Court does not suggest that Rule 41(b) is without force, it cannot be said, at least on these facts, that the violation at issue necessarily resulted in a constitutional infirmity. *See United States v. Schoenheit*, 856 F.2d 74, 77 (8th Cir. 1988) (Rule 41 and the Fourth Amendment are not coextensive).

In sum, the record as a whole demonstrates that, although the NIT warrant was issued in violation of Rule 41(b), that violation was not "of constitutional magnitude." *Skarda*, No. 15-3889, at *6. Indeed, the defendant has not established, much less argued, that the Rule violation in any way implicated the Fourth Amendment's fundamental requirements of probable cause, particularity, and neutrality. The Court therefore agrees with Judge Zwart's determination that the Rule 41(b) violation was not sufficiently fundamental to trigger exclusionary principles. *See filing 56 at 14*.

(b) Non-Fundamental Violation

The defendant next argues that even if the Rule 41(b) violation is technical or procedural in nature, suppression is appropriate under the prejudicial error test. As noted above, non-fundamental violations of Rule 41 may result in prejudice, thereby implicating exclusionary principles, if: (1) the search would not have occurred but for the violation of Rule 41, or (2) the investigators "recklessly disregarded proper procedure." *Welch*, 811 F.3d at 280-81. Here, the defendant contends that the Rule violation resulted in

prejudice because, without the NIT warrant, the government would not have obtained the defendant's IP address. And without the IP address, there would be no identifying information leading law enforcement to the defendant's home, and therefore, no evidence obtained from his residence. See [filing 60 at 10](#).

Magistrate Judge Zwart rejected this argument, concluding that the search "could have commenced even if the magistrate judge had determined Rule 41(b) prevented her from issuing the warrant." [Filing 56 at 16](#). This result, and the reasoning underlying it, is consistent with opinions from several federal district courts that have recently analyzed this issue. These courts have generally concluded that, even assuming a violation of 41(b), "an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant." [Jean, 2016 WL 4771096, at *18](#); see also, [Lough, 2016 WL 6834003, at *7](#); [United States v. Broy, 2016 WL 5172853, at *9 \(C.D. Ill. Sept. 21, 2016\)](#).

The defendant cites *United States v. Krueger* for the proposition that the government, under a prejudicial error test, "should not be allowed to argue in hindsight that they 'could have had' other ways of obtaining the warrant[.]" [Filing 60 at 10](#). In other words, the defendant suggests that the operative inquiry under the prejudicial error test is not whether the government, hypothetically speaking, could have obtained the warrant from some other magistrate or district court judge. Rather, courts must determine whether a federal magistrate judge could have complied with the Rule under the facts as they actually occurred. See [Krueger, 809 F.3d at 1116](#). And applying this standard, the defendant argues that he was clearly prejudiced because the Virginia magistrate judge could not, under the facts as they occurred, issue a search warrant for the defendant's home computer. See [filing 60 at 10-11](#).

While there is force to the Tenth Circuit's application of the prejudicial error test, the Court is ultimately convinced that the operative analysis—at least on these facts⁷—turns on whether the evidence obtained pursuant to the warrant "could have been available by other lawful means." [Michaud, 2016 WL 337263, at *7](#). And applying this analysis, the Court agrees with the Findings and Recommendation that, assuming the Rule 41(b) violation was

⁷ Importantly, the Tenth Circuit characterized the Rule 41(b) violation at issue as "clear and obvious." [Krueger, 809 F.3d at 1117](#). Although the defendant in this case suggests that the deficiency was similarly clear or obvious, the Court disagrees. As noted in the Magistrate Judge's Findings and Recommendation, the divergence in judicial opinions regarding the scope of the Virginia magistrate judge's authority under Rule 41(b) itself "provides ample evidence that under the facts of this case, there was nothing 'clear' about the magistrate judge's authority, or lack thereof." [Filing 56 at 19](#).

not of constitutional magnitude, the defendant failed to demonstrate prejudice. See [filing 56 at 16](#). Indeed, because the defendant does not argue that the warrant was facially deficient, there is no dispute that, had the same supporting documents been presented to a district judge in the Eastern District of Virginia, he or she would have signed the warrant.

3. GOOD FAITH

Even if a Rule 41(b) violation were to be of constitutional magnitude, or otherwise resulted in prejudice, suppression is not—in every instance—the appropriate remedy. Indeed, the exclusionary rule generally turns on the applicability of the good faith exception as set forth in *United States v. Leon*, 468 U.S. 897 (1984) and its progeny.

The defendant argues that the good faith exception does not apply in this case because the government officials seeking the approval of the NIT warrant "knew that they were asking a Magistrate Judge to authorize a search and seizure outside of their jurisdiction." [Filing 60 at 12](#). To support this argument, the defendant—in a conclusory manner—points to the pleadings and affidavits, which "make it clear" that law enforcement purposefully sought authorization for a search that they knew was prohibited under Rule 41. [Filing 60 at 13](#). The defendant also argues that the good faith exception does not apply in situations in which the issuing authority lacked legal authority to do so. See [filing 60 at 11](#).

Magistrate Judge Zwart found the defendant's arguments unavailing, and this Court agrees. As noted in the Findings and Recommendation, "[t]here is no evidence that the FBI misled [the magistrate judge in Virginia] when presenting the warrant application." [Filing 56 at 18](#). Further, the evidence in no way suggests that the magistrate judge in the Eastern District of Virginia "abandoned her judicial role" by either acting as a "rubber stamp" or failing to "read the warrant carefully." [Filing 56 at 18](#) (citing *Leon*, 468 U.S. at 914). Nor does the Court find, as the defendant suggests, that either law enforcement officers or the issuing magistrate acted in an objectively unreasonable manner in thinking that the NIT warrant was properly authorized under applicable rules and statutes. As Magistrate Judge Zwart notes, the divergence in judicial opinions on this issue provides sufficient evidence that, at a minimum, the magistrate judge's authority was not "clear" to law enforcement for purposes of the good faith exception. See [filing 56 at 19](#).

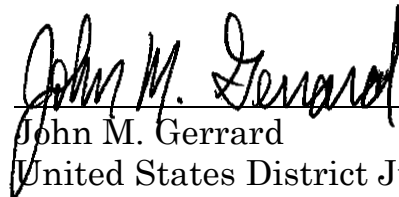
In sum, the Court agrees with Judge Zwart's finding that, even assuming exclusionary principles would apply, suppression is not the appropriate remedy on these facts. Accordingly, the defendant's motion to suppress will be denied.

IT IS ORDERED:

1. The defendant's objection ([filing 59](#)) to the Magistrate Judge's Findings and Recommendation is overruled.
2. The Magistrate Judge's recommendation ([filing 56](#)) is adopted.
3. The defendant's motion to suppress ([filing 37](#)) is denied.

Dated this 23rd day of December, 2016.

BY THE COURT:



John M. Gerrard
United States District Judge